Research Inventy: International Journal Of Engineering And Science
Vol.2, Issue 9 (April 2013), Pp 37-43
Issn(e): 2278-4721, Issn(p):2319-6483, Www.Researchinventy.Com

A Block Cipher Involving a Key Matrix and a Key bunch Matrix, Supplemented with Mix

[1,]Dr. V.U.K.Sastry, [2,] K. Shirisha
[1,2,]*Dept. of Computer Science & Engineering, SreeNidhi Institute of Science & Technology*

Abstract : *In this paper, we have developed a block cipher, which includes a key matrix and a key bunch matrix. In this, we have used the basic concepts of Hill cipher and the concept of the multiplicative inverse. This analysis is supplemented with a function, called Mix(), for creating confusion. The cryptanalysis carried out in this investigation firmly indicates that this cipher is unbreakable by all possible attacks, available in the literature.*

Keywords *- avalanche effect, cryptanalysis, decryption, encryption, key bunch matrix, key matrix.*

1. INTRODUCTION

The development of the the Hill Cipher [1], which involves a key matrix and the modular arithmetic inverse of the key matrix, has been a pioneering area of research in cryptography. The basic equations governing the Hill cipher are

$$C = (KP) \bmod 26, \textit{and} \tag{1.1}$$

$$P = K^{-1}C \bmod 26, \tag{1.2}$$

where K^{-1} is the modular arithmetic inverse [2] of the K. The K and the K^{-1} are related by the equation

$$(KK^{-1}) \bmod 26 = I, \tag{1.3}$$

where I is the unit matrix. Here mod 26 is used as attention is confined to the English alphabet, which contains 26 characters.

In the literature of the cryptography, it is well–known that this cipher can be broken by the known plaintext attack [2]. However, the recent literature is replete with a number of investigations [3-11], wherein the Hill cipher is modified and strengthened by introducing iteration, permutation and substitution. In the recent development of the cryptography, we have designed several block ciphers by introducing a key bunch matrix [12-18] in the process of the encryption and carried out the decryption by obtaining the multiplicative inverse of each key in the key bunch matrix. This cipher is strengthened by including the functions, namely, Mix(), Permute() and Substitute(), which alter the plaintext in each round of the iteration process.

In the present paper, our objective is to develop a block cipher which includes the basic ideas of the Hill cipher and the basic concepts of the block cipher which we have developed in the recent past. The strength of the cipher is expected to enhance significantly as we have blended the basic ideas of both the ciphers. Here, our interest is to see how the diffusion and the confusion of the binary bits, in each round of the iteration process, are enhanced by the superposition of one process (in the development of the block cipher) over the other.

Let us mention the plan of the paper. Section 2 is devoted to the development of the cipher. In this, we have presented the flowcharts and the algorithms pertinent to this cipher. In section 3, we have dealt with an illustration of the cipher and discussed the avalanche effect, which gives an idea about the strength of the cipher. Then we have carried out the cryptanalysis, in section 4. Lastly, in section 5, we have mentioned about the computations carried out in this investigation, and have brought out the salient features of this cipher.

II. DEVELOPMENT OF THE CIPHER

Consider a plaintext P, which can be written in the form of a square matrix of size n, given by

$$P = [\, p_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n. \tag{2.1}$$

As we have employed the EBCDIC code in writing this matrix, each element in this matrix lies in [0-255].
Let K be a key matrix given by

$$K = [\, k_{ij} \,],\ i=1 \text{ to } n,\ j=1 \text{ to } n, \tag{2.2}$$

Let us have an encryption key bunch matrix E, given by

E = [e_{ij}], i=1 to n, j=1 to n, (2.3)

The basic equations governing this cipher, which include the concepts of the modular arithmetic inverse and the multiplicative inverse, can be written in the form

P = (KP) mod 256, (2.4)

P = [$e_{ij} \times p_{ij}$] mod 256, i=1 to n, j = 1 to n, (2.5)

C = P, (2.6)

and

C=[c_{ij}]=[$d_{ij} \times c_{ij}$]mod 256, i=1 to n, j=1to n, (2.7)

C = (K^{-1}C) mod 256, (2.8)

P = C. (2.9)

Here, the equations (2.4) – (2.6) govern the encryption process, and (2.7) – (2.9) describe the decryption process. In the above equations, C denotes the ciphertext, and the e_{ij} and the d_{ij} are governed by the relation

($e_{ij} \times d_{ij}$) mod 256 = 1, (2.10)

It is to be noted that both e_{ij} and d_{ij} are odd numbers lying in [1-255], and each d_{ij} can be determined for the corresponding chosen e_{ij}.

The flowcharts depicting the cipher can be drawn as shown in Figs. 1 and 2.

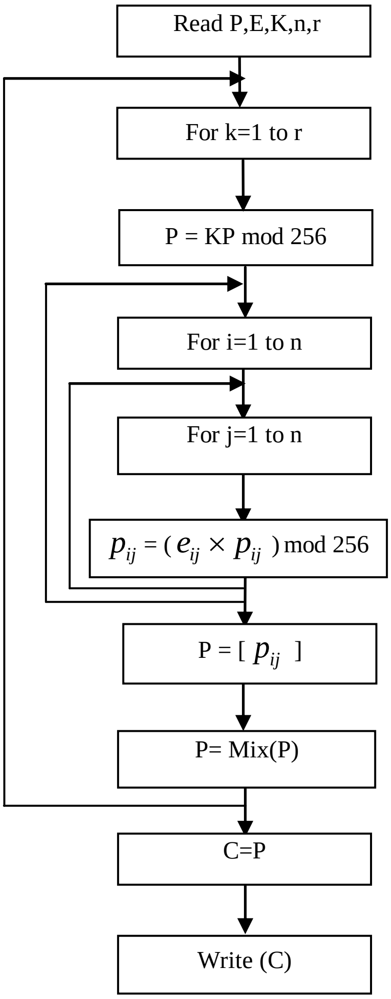

Fig.1 Flowchart for Encryption

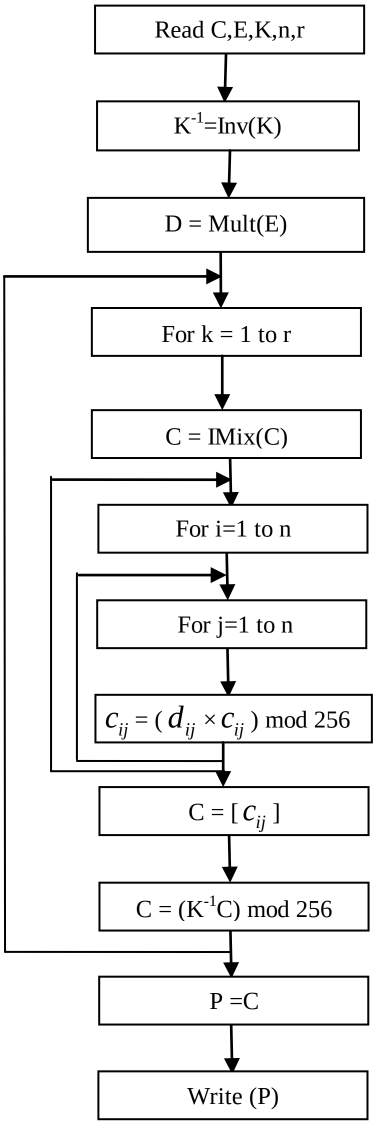

Fig.2. Flowchart for Decryption

The algorithms corresponding to the afore-mentioned flowcharts can be written in the form shown below.

2.1 Algorithm for Encryption

```
1.  Read P,E,K,n,r
2.  For k = 1 to r do
      {
3.   P = KP mod 256
4.  For i=1 to n do
      {
5.  For j=1 to n do
      {
6.  $p_{ij}$ = ( $e_{ij} \times p_{ij}$ ) mod 256
      }
      }
7.  P = [ $p_{ij}$ ]
8.  P = Mix(P)
      }
9.  C=P
10. Write(C)
```

2.2 Algorithm for Decryption

```
1.  Read C,E,K,n,r
2.  D=Mult(E)
3.  $K^{-1}$ = Inv(K)
4.  For k = 1 to r do
      {
5.  C=IMix(C)
6.  For i =1 to n do
      {
7.  For j=1 to n do
      {
8.  $c_{ij}$ = ( $d_{ij} \times c_{ij}$ ) mod 256
      }
      }
9.  C = [ $c_{ij}$ ]
10.  C=($K^{-1}$C) mod 256
      }
11.  P=C
12.  Write (P)
```

In the above flowcharts and the algorithms, r denotes the number of rounds in the iteration process. Here, we have the function Mix() in the encryption process. The basic ideas underlying in this function can be explained as follows.

Consider the plaintext P = [p_{ij}], i = 1 to n, j= 1 to n, in any round of the iteration process. On writing each element of this matrix in its binary form, we get a matrix of size $n \times 8n$. Let us now divide this matrix into 2 halves, wherein the first half is containing right from $(1)^{st}$ column to $(4n)^{th}$ column, and second matrix is containing $(4n+1)^{th}$ column to $(8n)^{th}$ column. We place the elements of $(4n+1)^{th}$ column after the 1^{st} column, the elements of the $(4n+2)^{th}$ column after the 2^{nd} column, etc., till we exhaust all the columns. Then, we write the binary bits, in terms of decimal numbers, by taking the binary bits in a column-wise manner. Thus we get a new matrix of size $n \times n$. This is the process in function Mix().

Imix() denotes the reverse process of Mix().

In the process of decryption, we having the functions Inv(), for obtaining the modular arithmetic inverse of a matrix, and the function Mult() for finding the decryption key bunch matrix D =[d_{ij}]. For obtaining the modular arithmetic inverse of a matrix, say A, we employ the equations

$$AA^{-1} = I \qquad (2.11)$$

and

$$A^{-1} = \left[\frac{A_{ji}}{\Delta}\right], \qquad (2.12)$$

where A^{-1} is the arithmetic inverse of A, and A_{ji} is the transpose of A_{ij}, in which A_{ij} is the cofactor of element a_{ij} of the matrix A.

From (2.11) and (2.12), we get

$$\left(A \times \left[\frac{A_{ji}}{\Delta}\right]\right) \mod N = I \qquad (2.13)$$

where N is a positive integer. On multiplying both the sides by a scalar quantity d, we get

$$\left(A \times \lfloor dA_{ji} \rfloor\right) \mod N = (I \times \Delta \times d) \mod N \qquad (2.14)$$

If we obtain d such that $(\Delta \times d) \mod N = 1$, then (2.14) can be written in the form

$$\left(A \times \lfloor dA_{ji} \rfloor\right) \mod N = I \qquad (2.15)$$

This shows that the modular arithmetic inverse of A, which may be denoted by B, can be written in the form

$$B = [\, dA_{ji} \,] \bmod N. \qquad (2.16)$$

In function Mult(), we make use of the relation (2.10) and obtain the decryption key bunch matrix D.

III. LLUSTRATION OF THE CIPHER AND THE AVALANCHE EFFECT

Consider the plaintext given below.

Dear Brother! I have seen your letter. Do never join in this profession as death is very close to every soldier at every instance in this service. Go for higher education. Do think of discovering some interesting scientific facts or try to invent something with all your ability. I know you are very intelligent and you can make your mark in your future career and get name and fame to our country. Do remember serving mother and father in their old-age is much more important and valuable than serving this country, which is very vast having several castes, having several religions, having several languages, having several political parties and not having any unity among people. Do forget that job. Be happy in your life. (3.1)

Let us focus our attention on the first 16 characters of the plaintext. Thus we have

Dear Brother! I (3.2)

On using EBCDIC code, (3.2) can be written in the form of a matrix P, given by

$$P = \begin{bmatrix} 196 & 133 & 129 & 153 \\ 64 & 194 & 153 & 150 \\ 163 & 136 & 133 & 153 \\ 79 & 64 & 201 & 64 \end{bmatrix}. \qquad (3.3)$$

Let us take the key matrix K and the encryption key bunch matrix E in the form

$$K = \begin{bmatrix} 210 & 71 & 87 & 152 \\ 255 & 161 & 164 & 181 \\ 218 & 64 & 59 & 177 \\ 228 & 255 & 204 & 148 \end{bmatrix} \qquad (3.4)$$

and

$$E = \begin{bmatrix} 21 & 221 & 13 & 197 \\ 45 & 67 & 143 & 149 \\ 87 & 205 & 197 & 1 \\ 253 & 255 & 9 & 67 \end{bmatrix} \qquad (3.5)$$

On using E and the concept of the multiplicative inverse, we get the decryption key bunch matrix D. Thus we have

$$D = \begin{bmatrix} 61 & 117 & 197 & 13 \\ 165 & 107 & 111 & 189 \\ 103 & 5 & 13 & 1 \\ 85 & 255 & 57 & 107 \end{bmatrix}. \qquad (3.6)$$

On making use of the plaintext P, the key matrix K, the encryption key bunch matrix E, and the algorithm for the encryption process, given in section 2, we get the cipher text C in the form

$$C = \begin{bmatrix} 60 & 12 & 110 & 22 \\ 153 & 113 & 179 & 69 \\ 250 & 114 & 230 & 81 \\ 171 & 40 & 159 & 212 \end{bmatrix}. \qquad (3.7)$$

On utilizing the C, the K and the D, and applying the decryption algorithm, we get back the plaintext P, given by (3.3).

Let us now study the avalanche effect. On replacing the 2nd row 2nd column element, 194 of the plaintext matrix P, by 226, we get a new plaintext matrix. On using this modified plaintext matrix, the K and the E, and applying the encryption algorithm, given in section 2, we get the corresponding ciphertext C in the form

$$C = \begin{bmatrix} 181 & 60 & 132 & 11 \\ 65 & 130 & 52 & 145 \\ 80 & 82 & 49 & 138 \\ 118 & 183 & 115 & 12 \end{bmatrix}. \qquad (3.8)$$

On comparing (3.7) and (3.8), after converting them into their binary form, we notice that these two ciphertexts differ by 70 bits out of 128 bits.

Let us now consider a one binary bit change in the key bunch matrix E. To this end, we replace the 1st row 4th column element, 197 by 196. On using this modified E, the original plaintext P, the key K and employing the encryption algorithm, we obtain the corresponding ciphertext in the from

$$C = \begin{bmatrix} 115 & 240 & 218 & 86 \\ 35 & 229 & 228 & 210 \\ 53 & 46 & 218 & 112 \\ 55 & 67 & 128 & 35 \end{bmatrix}. \qquad (3.9)$$

After converting (3.9) into its binary form, and comparing the resulting matrix with the binary form of (3.7), we find that these two differ by 71 bits out of 128 bits.

From the afore-mentioned results, we conclude that the avalanche effect is quite up to the mark and the strength of the cipher is expected to be very good.

IV. CRYPTANALYSIS

In the literature of cryptography, the strength of a cipher is a very important issue and this is decided by considering all possible attacks. The attacks that are considered are

1. Ciphertext only attack (Brute force attack),
2. Known plaintext attack,
3. Chosen plaintext attack, and
4. Chosen ciphertext attack.

Generally analytical proofs are offered for the first two attacks, and intuitive inspections are made for the latter two attacks. No cipher will be accepted unless it withstands the first two attacks. In this cipher, the key matrix and the key bunch matrix are square matrices of size n. Here it is to be noted that the key bunch matrix contain odd numbers which are lying in [1-255]. In the light of these factors, the size of the key space is

$$2^{8n^2} \times 2^{7n^2} = 2^{15n^2} = \left(2^{10}\right)^{1.5n^2} \approx \left(10^3\right)^{1.5n^2} = 10^{4.5n^2} \qquad (4.1)$$

If the time required for the execution of this cipher with one key matrix and one key bunch matrix is 10^{-7} seconds, then the time for the computation of this cipher with all possible keys in the key space is

$$\frac{10^{4.5n^2} \times 10^{-7}}{365 \times 24 \times 60 \times 60} = 3.12 \times 10^{4.5n^2-15} \; years. \qquad (4.2)$$

Here, in this analysis, as we have taken n=4, the time required for the whole computation is 3.12×10^{57} years. As this number is very large, we conclude that we cannot break this cipher, by the brute force attack. Let us now consider the known plaintext attack. In order to carry out this attack, we are provided with any number of plaintext and ciphertext pairs that we may require, in this process. If we confine our attention to only one round of the iteration process, that is taking r=1, the basic equations governing the cipher are

P = (KP) mod 256, (4.3)

P = [$e_{ij} \times p_{ij}$] mod 256, i=1 to n, j = 1 to n, (4.4)

P= Mix(P), (4.5)

and

C = P. (4.6)

Here, as C is known to us, we can determine P, occurring on the left hand side of (4.5). On using Imix(), we get the P on the right hand side of (4.5), and hence the P occurring on the left hand side of (4.4). Though the initial plaintext P occurring in the right hand side of (4.3) is known to us, we cannot proceed anymore and break the cipher in any way. As this is the case with r=1, we cannot break this cipher by the known plaintext attack, as we have taken r=16, in this analysis.

On inspecting the basic equations of this cipher, with all possible intuitions, we find that it is simply impossible to break the cipher either by choosing a plaintext or a ciphertext, in a selective manner.

In the light of the afore-mentioned discussions, we conclude that this cipher is unbreakable by all possible attacks, and is having enormous strength.

V. COMPUTATIONS AND CONCLUSIONS

In this investigation, we have developed a block cipher which includes a key matrix and a key bunch matrix. This cipher is supported by a function, called Mix(), wherein the binary bits are thoroughly mixed in each round of the iteration process.

The programs for the algorithms for the encryption and the decryption are written in Java.

The entire plaintext, given by (3.1), is consisting of 725 characters. Hence this is divided into 46 blocks, wherein each block is containing 16 characters. In the last block, we have included eleven 0s as additional characters, to make it a complete block. On using the K, the E, and the plaintext in each block, one after another, and employing the encryption algorithm, we have obtained the ciphertext corresponding to each block. Thus we have got the ciphertext corresponding to the entire plaintext. This is given by (5.1).In this analysis, we have noticed very clearly, that the cipher is strengthened very much, on account of the multiplication with a key, firstly, and with the multiplication with the key bunch matrix, subsequently. It may be noted here that this cipher can be extended with a key matrix of large size, and a key bunch matrix of the corresponding size, and then this analysis can be utilized in image processing of gray level images and color images.

REFERENCES

[1] Lester Hill, (1929), "Cryptography in an algebraic alphabet", (V.36 (6), pp. 306-312.), American Mathematical Monthly.

[2] William Stallings: Cryptography and Network Security: Principle and Practices", Third Edition 2003, Chapter 2, pp. 29.

[3] V. U. K. Sastry, S. Udaya Kumar, and A. Vinay Babu, "A large Block Cipher using Modular Arithmetic Inverse of a Key Matrix and mixing of the Key Matrix and the Plaintext", Journal of Computer Science, 2(9), 2006, New York, pp. 690-697.

[4] S. Udaya Kumar, V. U. K. Sastry and A. Vinay Babu, "An iterative Process Involving Interlacing and Decomposition in the Development of a block Cipher", International journal of Computer Science and Network Security, vol. 6, No. 10, October 2006, Seoul, South Korea, pp. 236-245.

[5] P10V. U. K. Sastry, V. Janaki, "On the modular arithmetic Inverse in the cryptology of Hill Cipher", Proceedings of North American Technology and Business Conference, September 2005, Canada.

[6] V. U. K. Sastry, N. Ravi Shankar, "Modified Hill Cipher with Interlacing and Iteration ", Journal of Computer Science, Science Publications, 3(11):854-859, 2007.

[7] V. U. K. Sastry, N. Ravi Shankar, "Modified Hill Cipher for a large block of plaintext with Interlacing and Iteration", Journal of Computer Science, Science Publications, 4(1):15-20, 2008.

[8] V. U. K. Sastry, Prof. D.S.R. Murthy, Dr. S. Durga Bhavani, "A Block Cipher Invloving a Key Applied on both sides of the plaintext", International Journal of Computer and Network Security (IJCNS), Vol. 1, No.1, pp. 27-30, Oct 2009.

[9] V.U.K.Sastry, Aruna Varanasi, " A Modified Hill Cipher Involving Permutation, Iteration and the Key in a Specified Position"(IJCNS) International Journal of Computer and Network Security, Vol. 2, No. 10, pp. 157-162, October 2010.

[10] V.U.K.Sastry, Aruna Varanasi, S.Udaya Kumar, "A Modern Hill Cipher Involving a Permuted Key and Modular Arithmetic Addition Operation", International Journal of Advanced Research in Computer Science Vol.2 No.1,pp.162-165, Jan-Feb 2011.

[11] Dr. V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp. 1-6.

[12] Dr. V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and Including Another Key Matrix Supplemented with Xor Operation ", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp.7-10.

[13] Dr. V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and Including another Key Matrix Supported With Modular Arithmetic Addition", in International Journal of Computer Applications (0975 – 8887) Volume 55– No.16, Oct 2012, Foundation of Computer Science, NewYork, pp. 11-14.

[14] Dr. V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key Bunch Matrix and a Permutation", accepted in International Journal of Computers and Electronics Research (IJCER).

[15] Dr. V.U.K. Sastry, K.Shirisha, "A Novel Block Cipher Involving a Key bunch Matrix and a Key-based Permutation and Substitution", accepted in International Journal of Advanced Computer Science and Applications(IJACSA). Nov 2012.

[16] Dr. V.U.K. Sastry, K.Shirisha, "A Block Cipher Involving a Key Bunch Matrix and an Additional Key Matrix, Supplemented with Modular Arithmetic Addition and supported by Key-based Substitution", accepted in International Journal of Advanced Computer Science and Application(IJACSA), Nov 2012.

60	12	110	22	153	113	179	69	250	114	230	81	171	40	159	212
43	93	44	112	25	8	52	0	111	204	109	126	139	228	61	109
14	111	120	232	238	32	224	172	244	78	197	0	40	172	250	199
56	60	8	104	131	44	68	31	87	1	154	236	168	219	233	185
214	1	44	16	179	224	143	239	176	104	93	129	69	175	66	17
94	138	25	101	243	151	214	207	10	184	28	155	112	235	80	183
179	197	62	108	145	40	122	93	114	71	177	92	127	196	59	141
208	64	112	111	139	72	102	87	63	91	85	91	1	26	227	58
234	76	70	36	237	231	115	187	141	245	26	228	148	114	235	181
243	84	72	132	93	233	248	154	255	189	72	209	101	33	104	0
143	143	169	101	141	79	103	141	128	91	144	203	80	229	179	171
189	19	114	242	220	0	174	246	247	35	72	58	232	95	116	147
155	243	35	15	88	211	11	178	244	241	186	25	215	30	166	29
130	35	230	61	121	70	239	220	90	126	173	50	161	219	202	159
116	196	138	157	153	236	144	173	62	231	34	104	8	50	45	202
56	36	1	164	40	222	151	242	194	43	241	8	53	253	131	211
185	235	30	64	5	178	58	125	124	17	241	72	13	189	17	83
28	131	195	52	211	191	92	225	187	175	162	115	215	57	36	66
89	102	100	231	26	11	104	103	225	45	16	82	55	187	50	189
248	77	208	203	227	189	72	255	26	129	151	83	197	231	207	230
153	161	248	203	102	131	214	111	120	43	200	116	248	150	2	167
41	112	62	43	68	47	169	90	238	29	4	187	79	133	235	96
241	194	105	166	183	131	127	148	39	30	249	181	91	156	6	211
1	112	251	216	209	139	216	21	63	3	54	248	202	231	148	107
235	61	95	115	250	237	105	92	35	149	167	164	37	226	28	146
193	74	152	2	105	96	235	85	216	210	243	135	186	146	86	210
153	89	96	23	121	168	0	45	58	151	51	190	220	120	180	8
5	32	234	201	102	74	21	113	87	79	199	214	80	186	112	84
220	162	37	134	4	101	115	209	35	213	121	197	166	67	150	72
150	29	134	70	185	83	30	227	76	186	30	39	156	46	26	185
13	248	146	220	13	115	178	210	195	134	40	159	195	132	222	71
208	214	165	19	137	113	38	1	14	86	43	128	217	240	96	249
11	244	10	168	113	90	178	18	237	227	123	100	244	142	54	175
247	104	210	139	233	239	40	106	124	97	167	228	75	9	2	178
94	149	60	238	99	17	228	194	171	83	207	210	44	204	19	92
198	245	156	200	79	226	81	6	100	185	24	81	102	198	27	19
214	190	241	145	37	250	15	214	151	193	236	195	167	137	216	148
20	1	225	229	14	56	99	80	146	182	77	65	238	149	186	70
149	107	168	187	90	92	234	115	9	99	22	10	12	176	185	203
13	157	155	133	223	141	59	124	178	239	83	189	240	117	20	60
248	139	170	102	252	39	111	179	195	49	126	134	192	187	217	101
57	123	141	191	174	46	164	249	101	165	212	136	55	251	64	124
73	251	35	111	103	12	32	137	99	50	47	160	68	213	15	96
201	188	74	51	143	241	248	168	212	173	194	211	233	19	134	18
50	153	0	95	242	161	39	102	59	225	180	39	175	36	107	227
251	121	200	61	108	125	155	138	194	140	161	103	243	27	130	150

(5.1)